Swedish Certification Body for IT Security

002 Evaluation and Certification

Issue: 35.0, 2023-Jun-02

Authorisation: Mats Engquist, Head of CSEC , CSEC

Table of Contents

1 Preface

1 This document is one of the governing documents for the Swedish Certification Body for IT Security (CSEC).

2 In this document, "the Scheme" refers to any or all of the Certification Schemes under which CSEC performs certifications and issues certificates.

3 This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. It is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of IT products for which security is a consideration, as well as those already involved in the Scheme, i.e. employees at the Certification Body, Evaluators, current customers, contractors, and security consultants.

4 The Scheme documents and further information can be obtained from the Swedish Certification Body for IT Security. Complete contact information is provided in the following box.

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: SE-115 88 Stockholm, Sweden
Visiting address: Banérgatan 62

Telephone: +46-8-782 4000 E-mail: csec@fmv.se
Web: www.csec.se

1.1 Purpose

5 This document describes the evaluation and certification process performed under the Scheme. The document provides detailed information about the evaluation and certification process and the responsibilities of each party involved in the process.

6 General information about the Scheme is published in External publications EP-001 *Certification and Evaluation - Overview*, and EP-301 *Certification and Evaluation – EUCC – Overview*.

1.2 Terminology

7 Abbreviations commonly used by CSEC are described in EP-001 *Certification and Evaluation - Overview.*

8 The following terms are used to specify requirements.

SHALL	Within normative text, “SHALL” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).
SHOULD	Within normative text, “SHOULD” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.
MAY	Within normative text, “MAY” indicates “a course of action permissible within the limits of the document.” (ISO/IEC).

CAN	Within normative text, “CAN” indicates “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).

2 Introduction

2.1 Overview

9 IT security evaluation is the process whereby an IT product or protection profile (PP) is assessed against a specific set of security requirement claims. IT security certification is the oversight of the evaluation process by a Certification Body. The objective of the evaluation and certification process is to perform an impartial, objective, and internationally standardised assessment of the IT product or protection profile, resulting in an internationally recognised certificate.

10 The Certification Body will produce a certification report (CR) and issue a certificate after a successful certification.

11 Evaluations may be carried out on an IT product that has already been developed, or in parallel with the development. The latter model is known as concurrent evaluation.

12 The IT product in both cases has a defined target of evaluation (TOE) on which the evaluation is targeted.

13 The Scheme supports both initial evaluations and assurance continuity (re-evaluations and certificate maintenance). An initial evaluation (called simply an *evaluation*) is based on a target of evaluation or a protection profile that has not previously been evaluated, while assurance continuity is performed on an already evaluated and certified target of evaluation.

14 In the discussion that follows, no distinction is made between a target of evaluation and a protection profile evaluation, although certain evaluation aspects do not apply to protection profile evaluations as described by the Common Criteria (CC).

2.2 Principles of Evaluation

15 The evaluation and certification process is designed to achieve appropriateness, impartiality, objectivity, repeatability, reproducibility, generation of sound results, cost-effectiveness, and re-usability.

16 The principles of evaluation are as follows.

- All parties involved in an evaluation SHALL perform their required tasks to a degree of rigour consistent with the guidance and requirements of the target evaluation assurance level (EAL).
- No party involved in evaluation SHALL have a bias toward or against any target of evaluation or protection profile being evaluated. Proper technical oversight coupled with a Scheme that eliminates conflicts of interest SHOULD reduce any residual bias to a nominal level.
- Individuals cannot be totally free of opinion or judgements; therefore, proper technical oversight based on well-defined methodology and interpretations SHALL be used to reduce opinions and judgments to an acceptable level.
- The results of each evaluator action element SHOULD yield the same result regardless of who performs the evaluation, and requirements SHOULD be interpreted in a consistent manner across evaluations.
- Outputs of the evaluation process SHALL demonstrate good judgement and an accurate technical assessment of the target of evaluation or protection profile. The evaluation process and results SHOULD be subject to technical oversight to ensure that the requirements of the CC, the Common Methodology (CEM), and the Scheme are met.

- A balance SHOULD continually be maintained between value, and expenditure of time and resources in the evaluation of target of evaluation s and protection profiles.
- The results of evaluating a target of evaluation or a protection profile, and the interpretations that arise in the course of the evaluation, SHOULD be useful in subsequent evaluations if the same conditions apply.

17 These principles are upheld by:

- using the CC, which provides a well-defined set of security requirements;
- using the CEM when assessing an IT product or a protection profile against the requirements; and
- implementing the evaluation and certification process defined by the Scheme.

2.3 Requirements for Certification

18 The Requirements for Certification are described in the following documents.

- The CC, and the CEM
- Supporting Documents authorised through the Common Criteria Recognition Arrangement (CCRA) and/or the Senior Officials Group, Information Systems Security - Mutual Recognition Agreement (SOGIS-MRA)
- International Interpretations
- The Scheme documentation

19 Procedures for introducing changes to the Requirements for Certification are described in EP-007 *Quality Manual*.

2.4 Standard Versions

20 The versions of the CC and the CEM used in certifications by the Swedish Certification Body for IT Security (CSEC) are those listed on the CC project website, www.commoncriteriaportal.org.

21 Final decision about which version is used in a Certification, and thus presented on the certificate and on the certification report, is made when the Certification Body makes the decision on certification.

22 Unless otherwise agreed with the Sponsor, the versions used should be the versions valid at the time of the final evaluation report (FER).

23 If the valid versions have been updated during the evaluation and certification, an impact analysis may have to be performed, and parts of the evaluation may have to be updated.

24 If the impact is too extensive, the certification may also be based on older versions of the standards, as long as this is consistent with the recommendations made by the CCRA.

2.5 Evaluation and Certification Process

25 The generic evaluation process has three distinct phases, which are explained in detail below.

1. Start-of-evaluation	The four parties involved in the evaluation and certification (Developer, Sponsor, IT Security Evaluation Facility - ITSEF, and Certification Body) prepare for evaluation.
2. Conduct of evaluation	The evaluation is performed.

3. Conclusion of evaluation The evaluation is completed.

2.5.1 Start-of-evaluation

26 The start-of-evaluation phase includes any activities relevant to the upcoming evaluation, including the following.

27 It is recommended that the ITSEF conduct a feasibility study before accepting the evaluation. The sponsor MAY provide the security target (ST) or the protection profile (PP), and possibly other evaluation evidence, to the Evaluator so that the Evaluator may determine the likelihood of a successful evaluation and the possible cost.

28 If the Sponsor decides to seek certification of the protection profile or IT product, the Sponsor contracts with an ITSEF to perform the evaluation and applies for certification with the Certification Body.

29 The Sponsor submits a signed application for certification to the Certification Body, including several documents, which together demonstrate readiness for the evaluation and certification process, and acceptance of the Sponsor responsibilities described in section 3, *Parties and Responsibilities*. The necessary documents may vary depending on the evaluation type.

30 The Certification Body performs an application review, including all attached documents, after which it decides whether to undertake, or decline, the Certification. If the decision is to undertake the certification, a Certification Agreement is established according to the procedures described in section 4.3.1, *Certification Agreement*.

31 During start-of-evaluation, the Developer/Sponsor carries out a number of activities to prepare for evaluation. The certification application and other necessary documents must be created. Start-of-evaluation tasks may be handled by the Sponsor/Developer alone, or may include independent pre-evaluation consultancy.

32 Pre-evaluation consultancy may be provided by the ITSEF performing the evaluation only if a possible conflict of interest is prevented by proper separation of evaluation and consultancy work.

33 For more detail on the Start-of-evaluation phase see section 4, *Start-of-evaluation*.

2.5.2 Conduct of Evaluation

34 After the Certification Body has approved the application, the evaluation may start. The Evaluators will carry out the evaluation in accordance with the agreed evaluation work plan (EWP). Usually the Evaluator begins with evaluation of the security target and then performs the evaluator actions as described in the CEM for the targeted evaluation assurance level, i.e., investigating the target of evaluation, the development environment, etc.

35 During the conduct of evaluation phase, the Developer submits evaluation evidence to the Evaluator at the ITSEF. The Evaluator uses the CEM to assess the evidence, and requests necessary updates in the evaluation evidence from the Developer, so that remaining issues with status FAIL or INCONCLUSIVE are avoided.

36 Thereafter the evaluation approach and results are documented in single evaluation reports. The single evaluation reports are submitted to the Certifier at the Certification Body, together with the evaluation evidence. The format and required content of the reports are described in Appendix C, *Single Evaluation Report.* Copies of the single evaluation reports are distributed to the Sponsor and to the Developer.

37 The evaluation work is divided into several parts, resulting in a series of single evaluation reports. For each single evaluation report, the Certifier will review the Evaluator's approach and results, and document any findings in a technical oversight report (TOR), which is submitted to the ITSEF. The Evaluator responds by updating the single evaluation report, preferably after the evaluation evidence has been updated, and submitting the changed documents to the Certifier. The process may be iterated.

38 The conduct of evaluation phase also includes site visit activities. The Evaluator and the Certifier visit the Developer site to assess whether procedures are being followed in a manner consistent with that described in the documentation. The Certifier may also be present during the Evaluator's independent testing.

39 During the whole process, the Certification Body oversees the evaluation, supports the evaluation as requested by the Evaluator, and responds to each evaluation report with a technical oversight report.

40 For more detail on the Conduct of Evaluation phase see section 5, *Conduct of Evaluation*.

2.5.3 Conclusion of Evaluation

41 After the Evaluators have assessed all necessary topics, all necessary single evaluation reports have been produced, and the Certification Body has reviewed and accepted them all, the conclusion of evaluation phase begins. The Evaluator produces a final evaluation report summarising all the findings and submits it to the Certification Body. The Certification Body assesses the final evaluation report, produces and publishes the certification report, and issues the certificate to the Sponsor. The certification report and the certificate itself will be issued in English, but can be issued in Swedish upon the Sponsor’s request.

42 For an evaluation of a protection profile a final evaluation report is not necessary. In this case the certification report is based on a single evaluation report for the assurance class protection profile evaluations (SER APE).

43 The Certification Body also exercises control over the use of the certificates issued. This is described in section 8.2, *Certificate Misuse.*

44 This phase also involves publishing the evaluation results as agreed with the Sponsor and in accordance with the requirements for mutual recognition.

45 For more detail on the Conclusion of Evaluation phase see section 6, *Conclusion of Evaluation*.

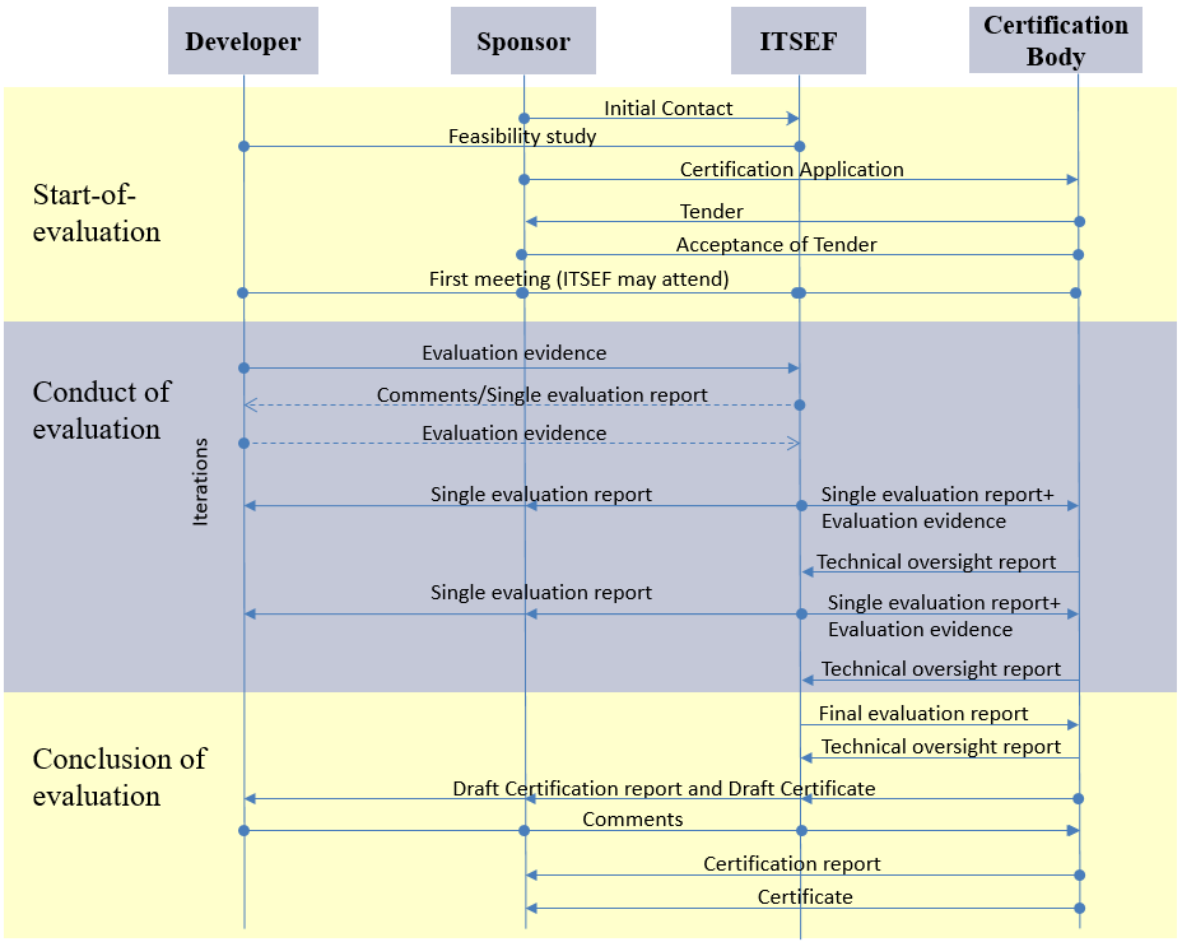

Figure 1 shows the four parties involved in the evaluation and certification process (Sponsor, Developer, ITSEF, and Certification Body), the phases of the process, and a simplified document delivery sequence.

2.6 Assurance Continuity

46 Assurance continuity provides the means to extend the scope of a Common Criteria certificate to cover an updated version of the certified product (more specifically the certified target of evaluation) without having to perform a complete certification.

47 Assurance continuity can be performed as *certificate maintenance* or as a *re-evaluation*.

48 *Certificate maintenance* is applicable when the changes to the certified target of evaluation, its IT environment and/or its development environment can be shown to have minor impact on the assurance baseline.

49 If the Developer cannot, or chooses not to, show that the impact of the changes is minor, a *re-evaluation* SHOULD be performed using applicable parts of the evaluation and certification process.

50 For more detailed information about Assurance Continuity see section 9 *Assurance Continuity Procedures.*

2.7 Cross Frontier Evaluation

51 Evaluations where work is performed in locations situated outside Sweden are subject to the regulations in EP-191 *Cross Frontier Evaluation*. Some Evaluation activities are required to be performed at a Swedish site, designated as a Critical Location, or at the Developer site, whereas other activities may be performed at a Foreign Location covered by the ITSEF license, subject to approval by the Sponsor and the Developer.

2.8 Official Languages of the Scheme

52 Evaluation reports, oversight reports, and certification reports may be written in Swedish or English.

53 Other languages may be used in evaluation evidence and other documentation related to the certification, but must be made available in either Swedish or English if required by the Certification Body.

2.9 Management of Confidential Information

54 Documents received or drawn up by the Certification Body are official documents ("*allmän handling*") and may be kept secret by the Certification Body only when it is required to protect the interests covered by articles in The Swedish Law on Publicity and Secrecy regarding:

- the security of the realm or its relationships with another state or international organisation;
- inspection, control, or other supervisory activities of a public authority;
- the prevention or prosecution of crime;
- the economic interests of the public institutions; and
- the protection of the personal or economic circumstances of private subjects.

55 For further details on legal protection of confidential information, how to make the Certification Body aware of confidentiality claims and procedures for exchanging confidential information with the Certification Body please contact the Certification Body.

3 Parties and Responsibilities

56 All parties involved in the evaluation and certification shall fulfil their roles and responsibilities as defined by the CC, the CEM, and the Scheme. It is, therefore, important that all parties are aware of their responsibilities in the Scheme before the evaluation and certification starts.

3.1 Sponsor

57 The Sponsor is the organisation that funds the evaluation and certification, applies to the Certification Body for certification, contracts with the ITSEF, and arranges for Developer participation. The Sponsor and the Developer may be the same.

58 The Sponsor SHALL have formal agreements with:

- the ITSEF for the evaluation, and
- the Certification Body for the certification.

59 The Sponsor SHALL ensure that evaluation evidence, training, support, and access to facilities is provided to the Evaluator. This MAY require an agreement with the Developer, as well.

60 In some instances, more than one Developer MAY be involved in an evaluation, for example, in cases where subcontractors are involved, or where different organisations are responsible for developing different components of the product. Under such circumstances, it is essential for the Sponsor to ensure the cooperation of all parties.

61 The Sponsor SHALL ensure that the Certifier is provided with evaluation reports, evaluation evidence, training, support, and access to facilities.

62 The Sponsor SHALL assign a point of contact for the evaluation and certification, which is the contact person to use for the other parties involved. This point of contact SHOULD be the recipient for all communication with the Sponsor within the scope of the evaluation and certification, including invoices and the certificate.

63 The Sponsor SHOULD assign a point of contact for external communication related to the evaluation and certification. The Sponsor SHALL ensure that the Certification Body is notified of any changes to the point of contact.

64 Upon successful certification, the Sponsor is responsible for archiving a reference copy of the target of evaluation as well as any and all evidence produced by the Sponsor or the Developer that has been used by the Evaluator or by the Certification Body to perform evaluation or certification activities.

65 The archived material SHALL be complete in order to enable the course of the evaluation and certification to be traced and re-confirmed. It SHALL be securely and accessibly archived for at least five years from the date at which the certificate is issued.

66 The archived material SHALL be made available to CSEC at request within seven working days.

3.2 Developer

67 The Developer is the organisation that produces the target of evaluation. The Developer supports the Sponsor during the evaluation by providing necessary documentation, technical know-how, and evaluation evidence. The Developer and the Sponsor may be the same.

68 All Developer requirements are in legal terms, requirements on the Sponsor with whom the Certification Body has an agreement. In practice, the Developer is the party who will need to take action to fulfil these requirements.

69 The Developer SHALL:

- assign a technical point of contact who the other parties can contact for target of evaluation support and clarifications;
- support the evaluation, for example, by educating Evaluators and Certifiers on the target of evaluation;
- develop and deliver evaluation evidence;
- respond to Evaluator and Certifier findings, for example, by updating or producing new evaluation evidence; and
- support the Evaluator during site visits, for example, by ensuring that the Evaluator has access to development areas and can interview key personnel.

70 If the Developer is distinct from the Sponsor, it may be necessary that the Developer and the Sponsor agree how to support the evaluation. At higher evaluation levels, extensive Developer documentation is required; if this documentation evidence is not delivered as scheduled, the entire evaluation could come to a stop.

3.3 ITSEF

71 The ITSEF is the organisation contracted to perform the evaluation. It is responsible for ensuring that the assessment performed is consistent with the CC, the CEM, and the Scheme.

72 An ITSEF must adhere to the following requirements.

- Observe all rules of the Scheme as laid down in the Scheme documentation and interpreted by the Certification Body
- Be accredited by an authorised accreditation body, in accordance with ISO/IEC 17025 or be directly appointed by the government
- Ensure that the status of each of its individual Evaluator is recognised by the Certification Body
- Keep the Certification Body informed about the progress of ongoing evaluations and about any changes that might influence its ability to fulfil the requirements of the Scheme

73 The ITSEF is subject to supervision by both the Certification Body and the accreditation body as appropriate to ensure that it meets its obligations.

74 The ITSEF and the Certification Body must be independent organisations.

75 The Evaluator is associated with an ITSEF and performs the assessment of the target of evaluation. The Evaluator provides the Certification Body with evaluation reports containing findings and verdicts, such as single evaluation reports and final evaluation reports.

76 ITSEFs prove their expertise and ability to conduct evaluations by obtaining a license to operate under the Scheme. The Evaluator proves his expertise to the Certification Body by achieving the status of Evaluator or Qualified Evaluator. For further information about the procedures for ITSEF licensing and Evaluator status achievement, see External publication EP-004 *Licensing of Evaluation Facilities*.

77 The Evaluator SHALL:

- comply with the principles of evaluation (see section 2.2, *Principles of Evaluation*) and the Scheme;
- determine which supporting documents (CCRA and SOGIS-MRA) that are applicable to the evaluation and use them accordingly;
- perform the evaluator actions required by the EAL; CC for Information Technology Security Evaluation, Part 3: *Security assurance requirements;* the CEM; and the Scheme;

- request evidence from the Sponsor or Developer and receive and safely store it, e.g., documentation, the security target, and the target of evaluation;
- perform the site visits required by the Scheme and the CEM;
- request and receive evaluation support as needed, e.g., target of evaluation training by the Developer and interpretations by the Certifier;
- provide and maintain evaluation reports;
- provide the Certifier with evaluation evidence;
- receive and take any necessary actions in response to the oversight deliverables from the Certifier; and
- document and justify the overall verdict and interim verdicts to the Certifier.

78 Note that this is not a complete list of all evaluator tasks and responsibilities. Also note that the term *Evaluator* in this document is gender- and plural non-specific and applies equally to an individual Evaluator or an evaluation team.

79 For each evaluation, the ITSEF SHALL:

- determine the competence needed in the evaluation team,
- assign Evaluators accordingly,
- assign one Evaluator to be the evaluation point of contact, and
- assign a Lead Evaluator who SHOULD be technically responsible for the evaluation.

80 If necessary, the ITSEF SHOULD augment the evaluation team with internal or external technical experts.

81 The individual Evaluator/evaluation team SHALL be technically competent for the assigned evaluation activities. The Lead Evaluator SHOULD ensure that personnel with the appropriate competencies are assigned for each evaluation activity. Note that an individual evaluator can be both the point of contact and the Lead Evaluator for an evaluation.

82 The Lead Evaluator SHOULD be a Qualified Evaluator. For more information, see External publication EP-004 *Licensing of Evaluation Facilities*.

3.4 Certification Body

83 The Certification Body provides independent confirmation of the evaluation results by overseeing the evaluation process. This oversight is performed by Certifiers working for the Certification Body. The Certification Body will carry out surveillance of the ITSEF operation through its day-to-day involvement in the evaluations performed by the ITSEF.

84 The Certifier oversees an evaluation by reviewing the evaluation reports produced by the Evaluator. The result is documented in technical oversight reports.

85 Witnessing the Evaluator's site visits at the Developer site is added for EAL 3 or higher, unless otherwise decided. The Certifier may also witness the testing of the product.

86 The Certifier also provides support to the Evaluator regarding Scheme matters, interpretations of the CC, etc.

87 To ensure uniform application of the CC, the Certification Body itself is being reviewed and audited according to the rules and regulations for accreditation as well as according to the regulations for applicable arrangements on mutual recognition of CC certificates. The use of publicly available interpretations to document clarifying statements made by the Certification Body is aimed at ensuring consistent and uniform use of the CC and the Scheme rules.

88 The Certifier will:

- perform technical oversight of evaluations;
- receive and review evaluation evidence and evaluation reports;
- provide oversight deliverables, e.g., technical oversight reports;
- support evaluations by providing Scheme and CC interpretations and guidance;
- disapprove the Evaluator's overall verdict and interim verdicts if they are not well-founded or not appropriate;
- document and justify the findings from the oversight; and
- document the certification results in a certification report, and issue a certificate.

89 Note that the list above is not a complete list of all certifier tasks and responsibilities. Also note that the term *Certifier* in this document is gender- and plural non-specific and applies equally to individual Certifiers and a certification team.

90 The Certification Body shall create conditions that ensure that evaluations conform to:

- the principles of evaluation (see section 2.2, *Principles of Evaluation*),
- the CC,
- the CEM, and
- the Scheme.

91 For each certification, the Certification Body will:

- assign one Certifier to be the certification point of contact, and
- assign a Lead Certifier to be technically responsible for the certification.

92 The individual Certifier shall be technically competent to perform the assigned certification activities. The Lead Certifier will ensure that personnel with the appropriate competencies are assigned for each certification activity.

4 Start-of-evaluation

4.1 Overview

93 The start-of-evaluation phase begins with the Sponsor contacting an ITSEF to initiate an evaluation of a target of evaluation or a protection profile. Before and during this phase, the Sponsor will prepare for the evaluation and certification process, possibly with the help of the ITSEF. After the Sponsor and the ITSEF have completed the necessary preparation, the Sponsor will submit a certification application to the Certification Body.

94 The Certification Body decides whether to approve the application. If approved, the Certification Body submits a Tender based on the complexity class and the EAL-level of the product to be certified. This Tender must be accepted in writing by the Sponsor, which brings the formal agreement to a conclusion.

95 The date when the Sponsor signed the tender is considered to be the start date for the evaluation.

96 Prior to the start of the certification, the Certification Body may invite all parties to a First meeting.

4.2 Feasibility Study

97 It is recommended that the ITSEF conduct a feasibility study before accepting the evaluation. It is also recommended that the Sponsor and the Developer prepare for the evaluation and certification.

98 After an initial contact between the Sponsor and the ITSEF, the Sponsor MAY provide the security target or the protection profile, and possibly other evaluation evidence, in draft or completed form to the ITSEF.

99 The ITSEF MAY conduct a feasibility study on the provided evidence to determine the likelihood of a successful evaluation, as well as to scope out the evaluation and to estimate the cost.

100 The ITSEF MAY inform the Certification Body that initial contact has been made with a potential Sponsor and the expected completion date of the feasibility study. With the knowledge of initial contact between the Sponsor and the ITSEF, the Certification Body can formulate appropriate resource plans in preparation for certifier activities during the start-of-evaluation phase.

101 The feasibility study will result in one of the following conclusions.

- The evaluation is not feasible and therefore will not be initiated.
- The evaluation is feasible, but only after additional preparation.
- The evaluation is feasible and may proceed without the need for any additional preparation.

4.3 Application for Certification

102 The Sponsor or the ITSEF on behalf of the Sponsor SHALL submit the following documents to the Certification Body.

- An application for certification using External publication EP-196 *Certification Application with Terms - Form* (Or EP-199 *Certification Application with Terms (FMV) - Form*, for customers within FMV). The Sponsor SHALL sign the application for certification.
- The security target (ST) or protection profile (PP)

- An evaluation work plan (EWP)
- A list of all applicable supporting documents with relevant versions indicated
- All documents referenced in the security target or the protection profile which are not publically available

103 Other appendices may be added as needed.

104 An Evaluator impartiality and independence justification may, if required, be submitted as an appendix to the Application, or on request from the Certification Body.

105 All the documents identified above are referred to as the certification application deliverables and SHALL be delivered with the application for certification. The certification application is considered complete when all the documents identified above have been delivered to the Certification Body in a finalised version or in a draft version that meets the requirements of the certification review process.

106 An Application fee will be invoiced according to EP-008 *Charges and Fees.*

107 An Application for certification is valid one year from the date it is received by the Certification Body.

108 By signing the application the Sponsor commits to the following, which are a part of the formal agreement (see section 4.3.1 *Certification Agreement*):

- to fulfil the requirements for certification, including implementing appropriate changes when they are communicated by the Certification Body;
- to make all necessary arrangements for the conduct of the evaluation and certification, including provision for examining documentation and records, and access to the relevant equipment, location(s), area(s) and personnel;
- in case the Sponsor is not the Developer:
  - to ensure the Developer's co-operation in the fulfilment of these requirements;
- to make claims regarding certification consistent with the scope of certification;
- not to use its product certification in such a manner as to bring the Certification Body into disrepute and not to make any statement regarding its product certification which the Certification Body may consider misleading or unauthorized;
- to comply with any requirements that may be prescribed in the product certification scheme that relate to the use of marks of conformity, and on information related to the product;
- to inform the Certification Body, without delay, of changes that may affect its ability to conform with the certification requirements; and
- to archive the evaluated product in its certified configurations and all Developer evidence as outlined in the configuration list which is valid at the end of the certification procedure for a time frame of 5 years.

109 The Sponsor agrees that the Certification Body archives all evidence provided, as well as the Certification Body 's internal files, based on the scheme regulation for archiving.

110 The Sponsor agrees to all responsibilities defined in the Scheme.

111 In addition, for evaluations at EAL 2 and above and for which the Sponsor and the Developer are different organisations, the Developer SHOULD agree in writing to provide necessary support to the Sponsor throughout the evaluation. The agreement SHOULD also cover:

- confidentiality between the Sponsor and the Developer,
- intellectual property rights, and
- responsibilities after a completed evaluation and certification.

112 Upon request by the Certification Body, the Sponsor-Developer agreement SHOULD be made available to the Certification Body during the review of the certification application.

113 The Sponsor-ITSEF evaluation agreement SHOULD cover:

- confidentiality between the Sponsor and the ITSEF;
- intellectual property rights;
- terms of payment; and
- how evaluation-related documentation, software, hardware, etc. shall be handled after the evaluation.

114 Upon request by the Certification Body, the Sponsor-ITSEF agreement SHOULD be made available to the Certification Body during the review of the certification application.

4.3.1 Certification Agreement

115 According to the rules and regulations for accreditation the Certification Body is required to have a legally enforceable Agreement for the provision of certification activities to its clients.

116 This Agreement is established as follows.

1. The Sponsor signs and submits an Application for Certification to the Certification Body, and thereby accepts compliance with the client's responsibilities, as defined in section 4.3, *Application for Certification*.
2. The Certification Body decides the fees for the certification depending on the complexity of the product to be certified and the EAL, and sends a Tender to the Sponsor.
3. The Sponsor sends a letter of acceptance of the fee and the terms of the Tender, in writing, to the Certification Body.

117 These three documents together form the Certification Agreement.

4.3.2 Security Target or Protection Profile

118 The security target or the protection profile SHALL comprise all major content items stated in CC Part 1 *Introduction and general model* and SHALL enable the Evaluator to determine that there are no obvious deficiencies preventing the certification from starting.

119 The quality of the security target or the protection profile is of the utmost importance for the subsequent evaluation and certification.

120 A submitted security target or protection profile SHOULD fulfil the following requirements.

- The scope and physical and logical boundaries of the target of evaluation SHALL be clearly identified and meaningful for an evaluation and for a potential customer of the target of evaluation.
- The security functional requirements (SFR) provided by the target of evaluation SHALL provide a meaningful set of security requirements for the intended use.

121 The security target must be clear and consistent. Clarifications on requirements on the security target are described in Scheme Note 18, *Highlighted Requirements on the Security Target*. It is recommended that these be taken into account as early as possible in the certification project.

122 If the evaluation and certification will be subject to mutual recognition, the final version of the security target or the protection profile will be public and, therefore, SHOULD not contain any information that is not suited for publication. In cases where the final version of the security target contains information that should not be made publicly available, a sanitised security target, called a security target lite, can be published instead. The security target lite (ST-lite) must be a real representation of the complete security target. This means that the security target lite cannot omit information that is necessary to understand the security properties of the target of evaluation and the scope of evaluation. The Sponsor SHOULD notify the Certification Body in writing if a security target lite will be developed.

4.3.3 Evaluation Work Plan

123 The ITSEF SHOULD, together with the Sponsor, produce an evaluation work plan based on information gained during the feasibility study. The evaluation work plan SHALL describe the schedule for the evaluation and the locations in which each evaluation activity will be carried out.

124 The evaluation work plan SHALL meet the requirements stated in Appendix A, Evaluation Work Plan; that is, the evaluation work plan shall be reasonable in terms of time, cost, and fulfilment of the CC, the CEM, and the Scheme.

125 At a minimum, the evaluation work plan SHALL cover the following.

- Resources
- Competence and training of the resources
- Parallel evaluation activities
- Evaluation evidence deliverances
- Dependencies between evaluation activities

126 The Evaluator SHALL present to the Certification Body a detailed description of the Evaluator's approach to performing the evaluation work including a detailed evaluation time schedule (see the detailed evaluation description requirements in Appendix A, Evaluation Work Plan). The detailed description can be documented as a part of the evaluation work plan, or as a separate document.

127 If the evaluation covers new evaluation areas such as new versions of the CC and the CEM, assurance levels EAL 5 or above, or technical areas new to the ITSEF (e.g. hardware, smart cards), the evaluation facility SHOULD, in writing, declare the Evaluator's competence with respect to the new areas and how the Evaluator has achieved this knowledge.

128 If new evaluation areas are covered this may result in additional interviews with the Evaluator and new assessment of the ITSEF site and equipment.

4.3.4 Evaluator Impartiality and Independence Justification

129 An Evaluator impartiality and independence justification SHALL be submitted with the Application or on request from the Certification Body, if there are specific circumstances that may affect the Evaluators' ability to act free from any undue internal and external commercial, financial and other pressure and influence that may adversely affect the quality of their work.

130 When members of the ITSEF have been involved in consulting activities or assisting the Sponsor with the development of evaluation evidence, the Evaluator impartiality and independence justification SHALL explain how the objectivity of the evaluation will be upheld. The justification SHALL demonstrate sufficient organisational separation between those individuals providing consulting and those conducting the evaluation.

131 An Evaluator impartiality and independence declaration MAY be stated e.g. within the evaluation work plan or any other document and may not have to be documented in a separate document.

132 If there are no specific circumstances as described above, the Evaluator MAY omit an Evaluator impartiality and independence justification. This may, for example, be discussed with the Certification Body during the First meeting.

4.4 Certification Application Review

133 The Certification Body will acknowledge the receipt of the certification application and provide an estimate to the Sponsor specifying how long the Certification Body will need to review and accept the application. When the certification application is complete, one or more Certifiers will be assigned the task of analysing the contents of the application.

134 The certification application review will consider all submitted certification application deliverables and, if applicable, the evaluation agreement and the agreements between the Sponsor and Developer.

135 The Certifier will examine all certification application deliverables to determine whether the deliverables, the ITSEF, and the assigned Evaluators meet the requirements stated in this section and the relevant appendices.

136 The Certifier will determine the competence needed in the evaluation team and assess the assignments made by the ITSEF.

137 The Certifier shall determine that there are no obvious deficiencies preventing the certification from resulting in a certificate and a certification report.

138 The Certifier shall present to the Sponsor and Evaluator any and all reasonable doubts found during the examination of the application that may hinder execution of the evaluation work plan with fulfilment of the CC, the CEM, and the Scheme. However, the certifier shall not be held responsible for the comprehensiveness of this reporting and of other issues that might be discovered later.

139 If the Certifier finds evidence (or evidence incompleteness) that shows beyond a reasonable doubt that the evaluation cannot be executed with fulfilment of the CC, the CEM, and the Scheme, the Certifier will reject the certification application.

4.5 Handling of the Certification Application

140 The Certification Body will review the agreement between the Sponsor and the ITSEF to ensure that the agreement does not contain any conditions that impact impartiality.

141 The Certification Body will ensure that the ITSEF and the Developer has signed security agreements, "*säkerhetsskyddsavtal, SUA*", with the appropriate Swedish governmental organisation if information regarding national security or foreign relations is likely to be handled during the certification. The Certification Body will also ensure that the Evaluators and Developers have security clearance at an appropriate level.

142 For EAL 2 and above, the Certification Body will review the agreement between the Sponsor and the Developer (if these are separate organisations) to ensure that the Developer will support the evaluation and certification.

143 Upon completion of the certification application analysis and resolution of any issues raised, the Certification Body will assess whether there are any obstacles to performing the certification.

144 The versions of the CC, the CEM, and interpretations to be used during the evaluation will be defined. The versions and interpretations should be the official versions and all published interpretations listed on the CC project website, www.commoncriteriaportal.org, at the time of the submission of the certification application. The Sponsor SHALL ensure that the security target or the protection profile is consistent with this decision.

145 The Certification Body will assign a Lead Certifier and other Certifiers as needed depending on the complexity of the evaluation. The Certifiers are responsible for conducting technical oversight of the evaluation activities carried out by the Evaluator.

146 The Certification Body may use external experts on technical issues during the technical oversight process. The rules and procedures for Certification Body use of external experts are described in External publication EP-007 *Quality Manual*.

4.6 Notification to NIAP

Before starting certifications where the sponsor (or the developer) has the intention that the certified product shall be listed on National Information Assurance Partnership's Product Compliant List (PCL), the Certification Body will notify NIAP.

This notification includes the product name, the vendor, evaluation start date, and the NIAP-approved PP/EP with which compliance is being claimed.

During the certification, and in order to get guidance in the certification work, the Certification Body may exchange information with NIAP as deemed relevant and necessary.

4.7 First Meeting

147 A First meeting is held to provide the parties involved in a certification with information about the certification process and the function of the Certification Body.

148 The meeting may take place any time after the application has been received by the Certification Body.

149 The First meeting MAY be performed at the Certification Body or at the critical location of the ITSEF.

150 The Certification Body, the Sponsor, the ITSEF, and for EAL 2 and above the Developer, SHOULD be represented at the First meeting.

151 The purpose of the First meeting is primarily too:

- give information to stakeholders in a certification about what a certification is, how the Certification Body works and what expectations Developers, Sponsors and Evaluators should have on how the certification work is performed
- describe how the Certification Body works with information and documentation and how the exchange of encrypted information should be handled
- find any outstanding issues that are important to resolve in order for the work in the evaluation and certification to progress as smoothly as possible

152 If technical issues have arisen during the application review, it is appropriate that these are addressed at the First meeting, in which case the Lead Certifier SHOULD participate. In this case the Lead Evaluator and the Developer's technical point of contact SHOULD also attend the First meeting.

153 If a First meeting isn't held, the Certification Body will send the information that is usually presented at this meeting to the Sponsor and the ITSEF.

154 If the evaluation is a trial evaluation, the Certification Body will inform all parties about the effects this will have on the process. See External publication EP-004 *Licensing of evaluation facilities* for more information on trial evaluations and ITSEF licensing.

4.7.1 ITSEF Preparation

155 The ITSEF SHALL be prepared to account for the evaluation work plan at the First meeting and SHOULD be prepared for questions regarding time schedule and project risks.

4.8 Certifier Project Planning

156 Based on the evaluation work plan delivered as a certification application deliverable, the Certification Body will plan its own corresponding activities. The Certification Body will inform the ITSEF in writing which meetings and evaluation work items the Certifier intends to observe, as well as when the Certification Body plans to perform technical oversight at the ITSEF and Developer facilities.

5 Conduct of Evaluation

5.1 Overview

157 The conduct of evaluation phase can begin when the preparation work in the Start-of-evaluation phase is finished. The Sponsor and/or Developer will provide evaluation evidence, the Evaluator will perform evaluation activities, and the Certifier will perform technical oversight activities. The conduct of evaluation phase ends when all single evaluation reports are completed by the Evaluator and accepted by the Certifier.

158 The date of the final version of the final evaluation report (FER), or, in the case of a PP evaluation, of the single evaluation report for the assurance class protection profile evaluation (SER APE), is considered to be the end-of-evaluation date.

5.2 Sponsor and Developer Activities

159 The Sponsor and/or the Developer SHALL provide the ITSEF and the Certification Body with evaluation evidence.

160 The Sponsor and/or Developer SHALL also be prepared to act on findings made by the Evaluator or the Certifier. The Evaluator or the Certifier MAY require the Sponsor and/or Developer to update the evaluation evidence or produce records to demonstrate use of processes relevant to the evaluation.

5.3 Evaluator Activities

161 The Evaluator SHALL generate evaluation reports; perform CEM work units; conduct site visits and independent testing, etc.; all in accordance with the CC, the CEM, relevant interpretations, and the Scheme.

162 The Evaluator's verdicts for work units, evaluator action elements, assurance components, and assurance classes are called interim verdicts and are documented in single evaluation reports. The interim verdict follows the evaluator verdict assignment rules defined in the CEM. An interim verdict SHALL be one of the following: PASS, INCONCLUSIVE, or FAIL.

163 The Evaluation reports SHALL contain information about any technical experts, other experts or Evaluator assistants who have contributed to the evaluation and it SHOULD be clarified in the report which parts they have contributed with.

5.3.1 Evaluation Report Generation

164 The Evaluator SHALL document, in single evaluation reports with supporting justification, the interim verdicts of all CC evaluator actions performed in accordance with the CEM. A single evaluation report covers a subset of all assurance packages for the evaluation.

165 The recommendation is to cover no more than one assurance class in each single evaluation report. For larger assurance classes such as assurance class development (ADV), each assurance family within the assurance class (e.g., ADV_TDS, assurance class development -target of evaluation design) can be covered in a separate single evaluation report, especially for higher EALs.

166 The Evaluator SHALL produce single evaluation reports using the evaluation evidence provided by the Sponsor and/or Developer. The structure and content requirements of the single evaluation reports are detailed in Appendix C, Single Evaluation Report.

167 For a target of evaluation, a separate single evaluation report SHALL be written for the assurance class security target evaluation (SER ASE) and, in the case of a protection profile evaluation, a single evaluation report for the assurance class protection profile evaluation (SER APE) SHALL be written. An ASE or APE single evaluation report MAY be divided into multiple assurance family single evaluation reports if the Evaluator finds it suitable.

168 The single evaluation reports SHALL be submitted to the Certification Body for the Certifier's technical oversight.

169 The individual single evaluation reports SHALL be considered provisionally complete until no certifier findings or requests for clarification remain in any single evaluation reports or in the final evaluation report.

170 The assurance class security target evaluation (ASE) SHOULD be the first assurance activity conducted. The security target is the basis for the whole evaluation, and it must be clear and consistent before successful assurance work can be performed on other evaluation evidence.

171 Due to the importance of the security target the Certification Body has chosen to highlight the importance of some important requirements on this document. These requirements may be found in Scheme Note 18 *Highlighted Requirements on the Security Target*.

172 The security target evaluation SHOULD be reported in a single evaluation report before other target of evaluation activities begin. The security target single evaluation report remains provisionally complete until the target of evaluation is complete. Findings during the evaluation may necessitate changes to the security target, impacting the previous security target evaluation results and possibly requiring a renewed security target evaluation.

173 During an evaluation, it may be necessary to evaluate some work units and entire assurance families several times. The need to repeat evaluation work arises when new or updated evaluation evidence becomes available, or when findings during the evaluation require changes to the evaluation evidence. Reassessment results are captured in an updated single evaluation report. Note that every dependent work unit SHALL either be reassessed or a sufficient justification SHALL be given as to why reassessment is not necessary.

174 If the Certifier identifies faults or requests clarifications in the technical oversight report, the Evaluator SHALL respond or correct, update, and resubmit the single evaluation report. The evaluator's actions SHOULD be performed without delaying overall progress on the evaluation and certification.

175 If the technical oversight report identifies faults or requests clarifications, for each issue identified, the Evaluator SHALL produce an answer containing the requested clarification or a description of and references to the changes made to the single evaluation report and any evaluation evidence. This SHALL be documented in a separate document submitted with the updated single evaluation report, if applicable.

176 The Evaluator and Certifier MAY meet to discuss the evaluation report and the content of the technical oversight report. It is particularly recommended to do so on two occasions:

- after the single evaluation report for the assurance class security target evaluation (ASE) and
- after the single evaluation report for assurance class development (ADV) but before testing.

177 For an evaluation of a protection profile a final evaluation report is not necessary and the single evaluation report for the assurance class protection profile evaluation (SER APE) will therefore be used as an input for writing the certification report instead of the final evaluation report.

5.3.2 Site Visit Assessment

178 The purpose of site visits at the Developer site is to determine whether the procedures described in the Developer documentation are followed. Site visits SHOULD be performed for evaluations at EAL 3 and above, as required by the CC. The CEM identifies the assurance families for which site visits are applicable or required: assurance class life-cycle support capabilities (ALC_CMC.3 or higher), life-cycle support delivery (ALC_DEL) and life-cycle support development security (ALC_DVS).

179 The decision not to perform a site visit is subject to Certifier approval. The Evaluator SHALL produce a separate document detailing a site visit plan for site visits planned in the evaluation work plan. The site visit plan SHALL demonstrate how the Evaluator plans to conduct the site visit.

180 The Evaluator SHALL invite the Certifier to attend the site visit well in advance of the scheduled date.

181 The Evaluator SHALL produce a site visit report documenting the outcome after conducting the site visit. The site visit report SHOULD be considered input for the single evaluation reports covering work units related to site visits.

5.3.3 Re-use of Site Visit Assessment Results

182 For new evaluations, where site visits recently have been performed in another evaluation, the following additional rules may apply.

183 If no substantial changes have been done to security relevant parts of the Developer's procedures, within a time period of 18 months, and if there are no further relevant sites to visit, apart from those already covered, the Evaluator MAY provide a rationale explaining why a renewed site visit is not necessary. Based on this rationale, the Certifier MAY conclude that a site visit is not necessary.

184 A site visit may be necessary if:

- due to sampling, all relevant sites have not already been visited
- in the new security target, the new target of evaluation has dependencies on the development environment that have not been completely covered in the previous assessment

5.4 Certifier Activities

185 During the conduct of evaluation phase, the Certifier oversees the evaluation. This oversight is based on three Certifier activities:

- examination of evaluation reports and evaluation evidence as documented in the various Evaluator reports,
- participating in the Evaluator site visit at the Developer site (only applicable to EAL 3 or above, unless otherwise decided), and
- participating in the Evaluator testing activities.

186 The Certifier will perform oversight and deliver technical oversight reports, according to the evaluation work plan and the agreed time plan.

5.4.1 Single Evaluation Report Technical Oversight

187 The Certifier will examine all single evaluation reports to determine whether they are technically sound and consistent with the requirements of the CC, the CEM, the relevant interpretations, and the Scheme. The single evaluation report content and structure requirements are defined in Appendix C, Single Evaluation Report.

188 The Certifier will examine the single evaluation reports to verify the evaluation conclusions and the analysis supporting those conclusions. The Certifier can use the evaluation evidence to verify the Evaluator conclusions.

189 The result of the examination of an evaluation report is documented in a technical oversight report produced by the Certifier and sent to the Evaluator. The technical oversight report shall provide the Evaluator with identified evaluation issues, comments, and requests for clarifications. Each issue and request will be uniquely identified. The issues reported might require Evaluator, Sponsor, and/or Developer actions.

190 When an issue is resolved in an updated evaluation report the Certifier will close it by stating "No further comments" in the technical oversight report.

191 If the Certifier has no further comments, the single evaluation report is provisionally accepted. However, new or updated evaluation evidence and findings during the evaluation that require changes to the evaluation evidence sometimes impact previous evaluation results, requiring work units to be reworked.

192 The Certifier will ensure that technical oversight reports are made available to the Sponsor and/or Developer in case Sponsor or Developer actions are required.

193 The appropriate party (Sponsor, Developer, or ITSEF) SHOULD resolve reported issues in a timely manner, not delaying overall progress on the evaluation and certification.

194 The Evaluator SHALL update the single evaluation report if work units are reworked and/or respond to the Certifier's comments by written statements in the technical oversight report. The Certifier will review updated single evaluation reports and consider evaluator statements in the returned technical oversight report, and issue a new or updated technical oversight report.

195 The Evaluator and Certifier MAY meet to discuss the evaluation report and the content of the technical oversight report. It is particularly recommended to do so on two occasions:

- after the single evaluation report for the assurance class security target evaluation (ASE) and
- after the single evaluation report for the assurance class development (ADV) but before testing.

5.4.2 Site Visit Oversight

196 The Certifier may attend site visits performed by the Evaluator. Site Visit oversight is performed at EAL 3 and above, unless otherwise decided. The purpose is for the Certifier to observe the evaluator actions.

197 The Certifier shall review the Evaluator's site visit plan and, if necessary, request an update.

198 The Certifier will focus on observing the Evaluator's compliance with the principles of evaluation (see section 2.2, *Principles of Evaluation*). For example, the Certifier shall verify that the Evaluator only collects evidence, and does not generate new evidence.

199 The Certifier will document observations accumulated during the site visit assessment in an internal report. The observations will be used to verify the Evaluator's site visit report, which documents the outcome of the site visit. The Evaluator's site visit report SHOULD be considered input for the single evaluation reports covering work units related to site visits. The Certifier will report issues, remaining from the site visit, in the technical oversight reports corresponding to those single evaluation reports.

200 As long as the Developer sites, the product type, and the Evaluator performing the site visit are familiar to CSEC, the Certifier MAY decide that no site visit oversight will be necessary.

5.4.3 Voluntary Test Planning Meeting

201 The Lead Certifier and/or the Evaluator may propose a voluntary test planning meeting. The meeting should take place at least five working days before the test monitoring and the penetration testing for the assurance classes tests (ATE) and vulnerability analysis (AVA).

202 The goal of the meeting is that the Evaluator presents and justifies their test plan in order to reduce the risk that further tests need to be carried out due to shortcomings in the planning stage.

203 Output of the meeting's is preparatory work for the review for the ATE and AVA reports. The test planning meeting is not a final review. The Lead Certifier assesses, on a case by case basis, if the test planning meeting is sufficient or if test monitoring is to be done too. The preliminary test plan should demonstrate that the Evaluators intentions are reasonable, but full compliance with CC and CEM will be verified by reviewing the assurance class tests (ATE) report. More details are described in Appendix B *Test Planning Meeting*.

5.4.4 Testing Oversight

204 The Certifier will observe Evaluator actions such as independent testing and penetration testing. Witnessing the evaluator's testing is added for EAL 3 and above, unless otherwise decided. Evaluator oversight provides the Certifier with an opportunity to verify the evaluator's conformance to the CC and the CEM.

205 Although oversight is primarily an observation activity, the Certifier sometimes has an opportunity to provide guidance in response to a request from the Evaluator, Developer, or Sponsor. In such cases, the Certifier will carefully consider the nature of the guidance requested, giving due consideration to its application as a Scheme-wide interpretation and to its formal distribution in accordance with interpretation procedures.

206 The Certifier will document observations accumulated during the testing oversight in an internal report. The observations will be used to verify the Evaluator's reports, which document the outcome of the tests. The Certifier will report issues, remaining from the testing oversight, in the technical oversight report s corresponding to those single evaluation reports.

6 Conclusion of Evaluation

6.1 Overview

207 The conclusion phase starts when all single evaluation reports have been completed and all the Certifier's comments on the single evaluation reports have been closed.

208 The Evaluator will produce the final evaluation report, which will be used as an input for writing the certification report.

209 For protection profile evaluations the final evaluation report is not necessary, instead the single evaluation report for assurance class protection profile evaluations (APE) will be used as input.

210 This phase will end with the Certification Body issuing, and possibly publishing, the certificate and a certification report.

6.2 Final Evaluation Report Production

211 The final evaluation report reports on all evaluation activities in all single evaluation reports, covering evaluations of the security target and the target of evaluation. The objective of the final evaluation report is to provide information necessary to produce the certification report, which provides practical information about the target of evaluation to the consumer.

212 The Evaluator SHALL produce the final evaluation report, which SHALL be based on the full set of accepted single evaluation reports, by compiling relevant information. For protection profile evaluations the final evaluation report is not necessary if the single evaluation report for assurance class protection profile evaluation (SER APE) contains the necessary information instead of the final evaluation report.

213 The Evaluator's result is documented with an overall verdict in the final evaluation report. The overall verdict is defined in the CEM and shall be either PASS or FAIL.

214 The content and structure of the final evaluation report SHOULD conform to Appendix D, Final Evaluation Report. The information content requirements are driven by the requirements stated in the CEM, and Scheme-specific requirements.

215 The final evaluation report SHALL include detailed information about the evaluation. This may be achieved by referencing the single evaluation reports.

216 With the exception of the detailed information, the final evaluation report SHALL provide the information necessary to produce the certification report and SHOULD be free of any information that is not suited to be copied into the certification report. The final evaluation report MAY fulfil the information content requirements by reference.

217 The Evaluator SHOULD send the final evaluation report to the Sponsor and/or Developer for review prior to submission to the Certifier. This review is especially important for certifications that will be subject to mutual recognition. The Sponsor and/or Developer review SHOULD ensure that the final evaluation report can be used for the generation of the certification report.

218 In addition, the Evaluator MAY assume that the Certifier is familiar with general principles of IT and IT security and need not elaborate on them unless it is appropriate to do so to provide a clear presentation.

219 The individual single evaluation reports, especially the security target single evaluation report, are not technically complete until the evaluation is complete; therefore, if needed, single evaluation reports SHOULD be updated.

6.3 Final Evaluation Report Review

220 The Certifier will examine the final evaluation report to determine that the requirements for information content and structure are satisfied. The correctness and completeness of the final evaluation report is important, as this document is the basis for the certification report.

221 The Certifier will always generate a technical oversight report in answer to the final evaluation report.

222 The technical oversight report identifies issues and requests clarifications regarding the final evaluation report, and will be sent to the Evaluator. The Evaluator may have to update one or more single evaluation reports to resolve the issues found during the final evaluation report examination.

223 Issues reported in the technical oversight report might require Evaluator, Sponsor, and/or Developer actions; if necessary, an updated final evaluation report and possibly updated single evaluation reports and evaluation evidence SHALL be produced and submitted to the Certification Body.

224 If the technical oversight report identifies faults or requests clarifications, for each issue identified the Evaluator SHALL produce an answer containing the requested clarification or a description of and references to changes made to the final evaluation report, and possibly single evaluation reports, and evaluation evidence. This response SHALL be documented in a separate document submitted with the updated final evaluation report, if applicable.

225 If the conclusion is that that there is a need for major changes to a single evaluation report, or if the evaluation evidence needs to be updated, the Certifier will send the evaluation and certification back to the previous phase, conduct of evaluation.

6.4 Certification Report Preparation

226 When there are no further comments on the final evaluation report (see section 6.3 *Final Evaluation Report Review*), the Certifier will produce a certification report. The Certifier will use the final evaluation report as the basis for the certification report.

227 For protection profile certifications the Certifier will use the single evaluation report for the assurance class protection profile evaluation (SER APE) as the basis for the certification report.

228 The Certifier will deliver a draft certification report to the Sponsor and the Evaluator for comment, indicating a due date for comments. The Sponsor SHALL assist the Certifier by reviewing the certification report.

229 If the certificate is intended to achieve mutual recognition, the certification report shall only contain information that can be made public. The Sponsor SHALL inform the Certifier of any information in the certification report considered inappropriate for public release.

230 The Certifier will inform the Sponsor if suggested changes might have an impact on the Scheme compliance or mutual recognition. The Certifier shall also inform the Sponsor about the possibility of developing a security target lite.

231 If a security target lite is developed, the certification report will refer to the security target as well as to the security target lite, even if only the security target lite is published.

6.5 Certificate Report and Certificate Issuing and Publishing

232 The final version of the certification report will be distributed to the Sponsor.

233 A certificate may be issued when the overall verdict for an evaluation is PASS and when the requirements for certification, as stated in the Scheme, are fulfilled.

234 If a certificate has been issued, the Certifier will update the certified products list in accordance with the scope of recognition.

235 A security target or a protection profile that is certified, and should be internationally recognised, will be registered. The registration is the publication of the security target or the protection profile, and the registration identifier is the certification ID.

6.6 Cancelled Certifications

236 A certification may, upon request by the sponsor, be cancelled at any time during the evaluation and certification effort.

237 The request to cancel SHALL be sent in writing to the Certification Body and will be acknowledged at reception.

238 When a certification is cancelled, the Certification Body may invoice a fee corresponding to the amount of work performed by the certification body. This fee will not be higher than the agreed fixed price for the certification.

6.7 Project Clean-up and Closedown

239 After the evaluation has been finished, the Evaluator SHALL handle all material used during the evaluation according to the terms in the evaluation agreement; material will be archived, returned, or destroyed, as agreed.

240 The Certification Body will archive the reference material needed to demonstrate the certification results and how the certification was performed.

7 Certificate Validity within CCRA and SOGIS-MRA

241 Effective 1 June 2019, the validity of Common Criteria Certificates mutually recognised within the CCRA and SOGIS-MRA will be limited over time.

242 The validity period will be no more than 5 years from the date of certificate issuance.

243 The details of this policy may be found in the *Procedure for Certificate Validity* that may be obtained from the CCRA portal (www.commoncriteriaportal.org).

7.1 Valid Certificates

244 Valid certificates will be published on the Certified Products List (CPL) on the CCRA portal and on the list of valid certificates at the CSEC website.

7.2 Expired Certificates

245 Certificates with an expired validity period will be moved to an Archive list on the CCRA portal and to the list of Archived certificates at the CSEC website.

7.3 Surveillance/Reassessment

246 Procedures for surveillance/reassessment that allows for extending the administrative validity of a certificate according to the procedures approved by CCRA will be established by the Certification Body.

8 After a Certificate has been Granted

8.1 Duration and Validity of a Certificate

247 A certificate is valid only for the specific product and version that has been evaluated according to the Certification Report.

248 For as long as the certificate is valid, the Sponsor SHALL keep a reference copy of the target of evaluation.

249 For as long as the certificate is valid, the Sponsor SHALL also:

- keep a record of all complaints made known to the Sponsor relating to a product's compliance with requirements for certification and make these records available to the Certification Body when requested
- take appropriate action with respect to such complaints and any deficiencies found in products or services that affect compliance with the requirements for certification
- document the actions taken

250 The period of validity is agreed between the Sponsor and the Certification Body. During the period of validity, the certificate will be surveyed on a yearly basis to ensure that the Sponsor fulfils its obligations.

8.2 Certificate Misuse

251 The Certification Body exercises control over the use of associated trademarks and issued certificates.

252 The Certification Body will take appropriate administrative, procedural, or legal steps to prevent or counter misuse of certificates or associated trademarks and to correct false, misleading, or improper statements about certificates or about the Scheme.

253 Conditions for the use of trademarks applicable to the certification process are listed in External publication EP-070 *Conditions for Use of Trademarks*

254 The Certification Body will withdraw certificates in cases where the conditions for holding a certificate no longer apply.

8.3 Certificate Surveillance

255 After a successful certification, the Sponsor and the Certification Body can agree on surveillance of the certificate.

256 The surveillance period is agreed between the Sponsor and the Certification Body. The recommended period is five years.

257 During this period the Sponsor SHALL fulfil the requirements for validity of the certificate described in section 8.1 *Duration and Validity of a Certificate*.

258 The Certification Body will perform surveillance activities to ensure that the conditions for the validity of the certificate are continuously satisfied.

259 The surveillance can be performed in different ways: Planned inspection, unannounced inspection or self-declaration by the Sponsor.

Planned inspection

260 The Certification Body performs a planned and announced Site Visit at the Sponsor's premises and conducts the inspection. This is the normal way to perform the surveillance during the first year of the surveillance period.

Unannounced inspection

261 The Certification Body performs an unannounced Site Visit at the Sponsor's premises and conducts the inspection. Unannounced inspections may also be carried out on suspicion that the Sponsor does not fulfil its obligations.

Self-declaration by the Sponsor

262 The Sponsor makes a self-declaration and sends it to the Certification Body. This will be the yearly procedure after the Site Visit performed during the first year.

9 Assurance Continuity Procedures

9.1 Introduction

263 This chapter defines an approach to assurance continuity that is in accordance with the procedures agreed for mutual recognition under CCRA. Assurance continuity provides the means to extend the validity of a Common Criteria certificate to an updated version of the certified product (more specifically the certified target of evaluation) without having to perform a fully new certification.

264 The requirements and procedures for assurance continuity described in this document are based on the CCRA document *Assurance Continuity: CCRA Requirements*.

265 Where nothing else is specifically stated, the procedures and requirements in the CCRA-documents are applicable to Assurance Continuity also in the Swedish Common Criteria Evaluation and Certification Scheme.

9.2 Scheme-specific Requirements

266 In addition to the requirements stated in *Assurance Continuity: CCRA Requirements*, Version 2.1, the following scheme-specific requirements may apply:

- Preparation of the impact analysis report (IAR) and application for certificate maintenance or re-evaluation SHALL be made by an ITSEF, licensed by the Certification Body, contracted by the Developer/Sponsor.
- Additional criteria for when changes to the certified target of evaluation are considered to be minor may be issued by the Certification Body. Such criteria may be issued as Scheme Notes and may be changed at any time.

9.3 Assurance Continuity Process

267 An overview of the assurance continuity process is shown in Figure 2

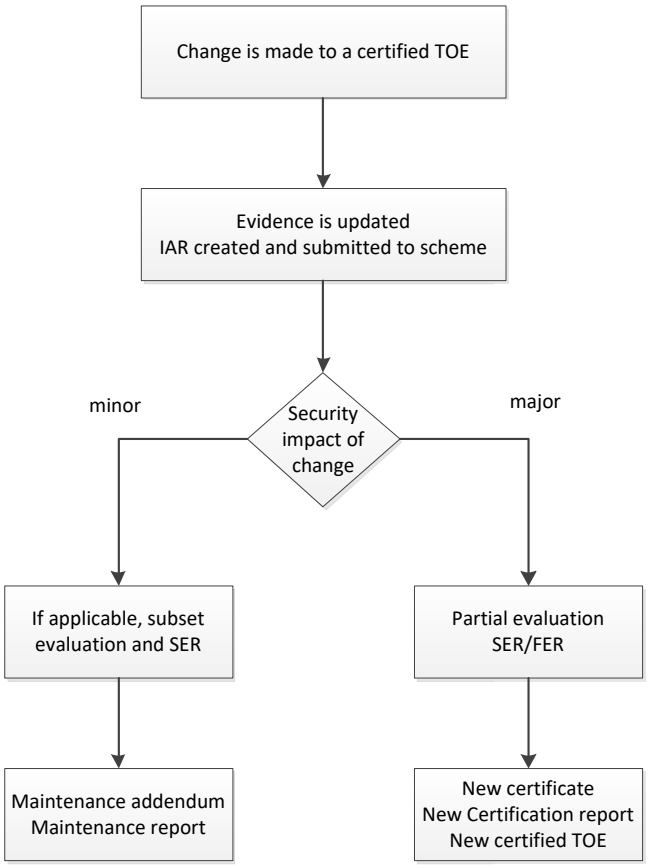

Figure 2 - The Assurance Continuity process, Abbreviations used in figure: target of evaluation (TOE), impact analysis report (IAR), single evaluation report (SER), target of evaluation (TOE), final evaluation report (FER)

9.3.1 Application

268 The start-up of the assurance continuity process is similar to that of a normal evaluation and certification process. The ITSEF on behalf of the Sponsor SHALL submit to the Certification Body:

- an application for maintenance or re-evaluation using External publication EP-196 *Certification Application with Terms - Form* (Or EP-199 *Certification Application with Terms (FMV) - Form*, for customers within FMV)
- impact analysis report (IAR)
- the certified security target
- if re-evaluation: an evaluation work plan (EWP)
- if there are specific circumstances, an Evaluator impartiality and independence justification.

269 All the documents identified above are referred to as the assurance continuity application deliverables and SHALL be delivered with the application for maintenance or re-evaluation. The application is considered complete when all the documents identified above have been delivered to the Certification Body in a finalised version or in a draft version that meets the requirements of the certification review process.

270 The impact analysis report SHALL be established by an IT Security Evaluation Facility (ITSEF) licensed within the Swedish Scheme, and the application SHOULD be sent to the Certification Body by this ITSEF.

271 The content requirements for the impact analysis report are described in Appendix E Impact Analysis Report .

272 If the application is for a re-evaluation, the description of the changes to the certified target of evaluation should focus on the changes in Developer evidence and the consequent scope of the re-evaluation.

273 For certificate maintenance, a Maintenance Impact Analysis Report (MIAR) shall be provided, where each change made to the target of evaluation should be individually described in such detail that it is easy to see whether the change is minor or major, and for each such change it should be concluded whether the change is minor and according to which criterion. The criteria for identification of minor and major changes are explained in the CCRA supporting document “Certificate Maintenance”.

Additional requirements for Certificate Maintenance applications

274 CSEC will only accept applications for certificate maintenance if the following additional requirements are met:

- No new target of evaluation models are accepted (relative to the base certification).
- If several consecutive updates are covered in a Maintenance Impact Analysis Report, they will be treated as several maintenance applications and multiple maintenance fees. For example, if the base target of evaluation (TOE) is version 3.0, simultaneous maintenance of the two consecutive versions 3.1 and 3.2 will count as two maintenance applications.
- Maximum 30 changes in the target of evaluation are accepted. Note that a functional update to a component within the target of evaluation which results in 25 changes in its source code, will count as 25 changes to the target of evaluation (i.e. not only one).
- The targets of evaluation subject to certificate maintenance SHALL be tested, and the scope of the tests both with regard to tested functionality and with regard to coverage of product variants SHALL be at least the same as in the original evaluation.

275 The general requirements in this document and those issued by CCRA (the supporting document “Assurance Continuity”) apply.

9.3.2 Application Reception and Review

276 An application fee will be charged upon reception of the application, see EP-008 *Charges and Fees*.

277 The Certification Body will review the application and may require additional or changed documents to be delivered.

278 Based on the results of the application review, the Certification Body will determine

- Whether the reported changes to the certified target of evaluation are to be considered minor or major, i.e. whether certification maintenance or re-evaluation will be performed
- The proposed fee for the certification maintenance or re-evaluation, which will be charged after completion of the assurance continuity project
- When the project can be started

9.3.3 Certificate Maintenance

279 If the development environment has been changed, the Evaluator will perform a subset evaluation and submit a report.

280 The Certifier will review the maintenance impact analysis report (MIAR) and other submitted documents to confirm that the changes made to the certified target of evaluation and/or the development environment have not adversely affected the assurance baseline.

281 The Certifier will then publish a Maintenance Addendum and a Maintenance Report in the list of certificates issued by CSEC on www.csec.se.

282 The Maintenance Addendum serves to include the changed version of the target of evaluation in the original certificate.

283 The Maintenance Report is based on the impact analysis report and is considered an addendum to the original certification report.

284 Maintenance MAY be performed within 2 years beyond the certification date.

285 The Certification Body may, as circumstances warrant, either lengthen or shorten this maintenance period, based on the IT product type and the needs of the consumer.

9.3.4 Re-evaluation

286 Re-evaluation is performed in the same way as a complete evaluation taking into consideration only those components determined to be affected by the changes.

287 The Evaluator submits one or several evaluation reports. The Certifier will review these and prepare a technical oversight report.

288 After concluded evaluation, the Certification Body will issue a new certificate and certification report for the changed target of evaluation.

289 This changed target of evaluation becomes the updated basis for any future changes that might be made.

10 Supporting Processes

10.1 Observation Report Handling

290 The observation report (OR) is a mechanism whereby actions required of an evaluation or certification party are documented and under control, to be resolved in a timely manner.

291 Observation reports may be used when a party experiences difficulties related to the evaluation, or with evaluation findings, such as:

- difficulties in obtaining necessary documentation from the Sponsor, Developer, or the ITSEF as scheduled in the evaluation work plan
- exploitable vulnerabilities, or incomplete or inaccurate evaluation evidence, leading to a potential evaluation failure
- unexpected delays to the evaluation work plan.

292 For example, if during the course of the evaluation, the Evaluator requires support from the Certifier that cannot be provided using other means, e.g., evaluation reports, the Evaluator may submit an observation report to the Certification Body.

293 The party responsible for resolution of an observation report SHALL resolve the matter in a timely manner, in accordance with the timeframe that SHALL be specified in the observation report. In cases where the specified timeframe cannot be met, the responsible party SHALL communicate this information and SHALL provide a revised timeframe for resolution.

10.2 Document Management

294 If a specific statement is identified in the Scheme procedures regarding the format of a certain document, this statement SHALL be followed. If no specific format statements apply, the documents SHOULD be in the Portable Document Format (PDF) and in digital form, preferably on CD/DVD. If a document is delivered to CSEC in multiple formats, one of these will be selected as the original. If one of these formats is consistent with the above format rules, that format will have precedence.

295 All evaluation reports and other Evaluator-generated documentation submitted to the Certifier in the certification process SHOULD be made available in two versions: one without change marks and one with change marks indicating all changes since the previous version. The version without change marks will have precedence.

296 Note that when submitting more than one document at a time to CSEC (whether by mail or electronically) these documents SHALL be accompanied by a covering letter at least including a list of the enclosed documents/files and the identity of the project/s to which the documents/files belong.

Appendix A Evaluation Work Plan

A.1 Overview

297 The evaluation work plan is a project plan that describes the evaluation work items, the work schedule, and the resources assigned to perform the evaluation work items. The evaluation work plan SHOULD be produced jointly between the Sponsor and the Evaluator, and SHALL be delivered as a part of the certification application deliverables to the Certification Body.

298 The Evaluator SHALL present a detailed evaluation description to the Certification Body. This SHALL be a part of the evaluation work plan or a separate document. At the end of this appendix are the requirements for the detailed evaluation description.

299 There are no requirements for the evaluation work plan structure. The requirement sections below groups similar requirements together.

A.2 General Requirements

300 The evaluation work plan SHALL demonstrate to the Certification Body that the plan is reasonable in terms of time, cost, and fulfilment of the CC, the CEM, and the Scheme. Typical areas of interest are: resources, resources' competence and training, parallel evaluation activities, evaluation evidence deliverances, and dependencies between evaluation activities.

301 The evaluation work plan SHALL, as in all other deliverables, contain appropriate protective markings and SHALL identify all appropriate evaluation identification information including, but not necessarily limited to: identification of the protection profile or the target of evaluation, Developer, Sponsor, ITSEF, and the protection profile or the target of evaluation version number.

302 The evaluation work plan SHALL describe, when applicable, how access is given to equipment (test systems, hardware, software, etc.) not owned by the ITSEF that is required for certain evaluation work. The Evaluator's independent tests may, for example, be performed in a lab at the Developer site.

A.3 Evaluation Activities

303 The evaluation work plan SHALL address all CEM general evaluation tasks, activities, and sub-activities matching the assurance requirements expressed in the security target.

304 The evaluation work plan SHALL address the production of the single evaluation reports and the final evaluation report, and SHALL also identify the evaluation evidence that is necessary to produce each of these reports. This can be checked by comparing each evaluation work item comprising the evaluation work plan with the input section for each CEM sub-activity for the corresponding assurance requirements, to verify that there are no evaluation evidence items missing from the evaluation work plan.

305 The evaluation work plan SHALL take proper account of all dependencies between work units. As an example, work units corresponding to vulnerability analysis MAY generally be the last ones scheduled, because vulnerability analysis relies upon Evaluator knowledge and experience gained as a result of performing the other evaluation work units.

A.4 Schedule and Delivery Dates

306 The evaluation work plan SHALL include an evaluation schedule that identifies the start date and completion date for each work item. The schedule MAY be represented as a Gantt chart and a delivery timetable.

307 The Sponsor and the Evaluator SHALL specify their deliveries and delivery dates in the evaluation work plan, and for EAL 2 and above the evaluation work plan SHALL include the Developer's delivery dates for the evaluation evidence.

308 For an evaluation at EAL 3 and above, the evaluation work plan SHALL schedule the Evaluator's site-visit(s) at the Developer facility or facilities. For EAL 3 and above, the Certification Body will also perform site-visits, i.e., Testing Oversight (a site-visit at the ITSEF or Developer site during independent and penetration testing) and site-visit (witnessing the Evaluator's site-visit at the Developer site), unless otherwise decided.

309 A site visit plan SHALL be delivered to the Certification Body at least five working days prior to the Evaluator's site-visit.

310 The Evaluator's test plan and vulnerability analysis, together with the Developer's test report SHALL be delivered to the Certification Body at least five working days prior to the Evaluator's independent and penetration testing.

311 The evaluation work plan SHALL identify planned meetings between the Evaluator and the Sponsor, Certifier, or Developer.

312 The evaluation work plan SHALL reserve time for updates of evaluation reports and evaluation evidence. The initial delivery of an evaluation report is usually not the only delivered version, because the Certifier might find issues with the report, or the evaluation evidence on which the report is based might change during evaluation and certification. Sometimes significant changes to the evaluation report, as well as to the related evaluation evidence, will be required.

313 Note that the single evaluation report SHOULD only be sent to the Certification Body when all the verdict in the single evaluation report is PASS or when there are unsolved FAIL or INCONCLUSIVE verdicts that require special attention from the Certifier.

314 For an evaluation of the target-of-evaluation, the assurance class security target evaluation (ASE) SHOULD be the first assurance activity planned.

A.5 Evaluation Staffing

315 The evaluation work plan SHALL identify the individual Evaluators assigned to each evaluation report, so that the Certifier can verify the following.

- The CEM principle of impartiality is upheld in cases where an evaluation is preceded by advice activities or other consultancy activities by the ITSEF.
- Evaluators are qualified to perform the assigned evaluation work.

316 Any technical experts, other experts or Evaluator assistants who are assigned to contribute to each evaluation from the beginning SHOULD be identified.

A.6 Evaluation Locations

317 The evaluation work plan shall denote the location where each evaluation activity is performed.

318 Unless otherwise has been agreed with the Certification Body, evaluator testing activities associated with the assurance classes tests (ATE) and vulnerability analysis (AVA) SHALL be performed at a Critical Location or at the Developer site. (See EP-191 *Cross Frontier Evaluation*.)

319 Evaluation activities SHOULD be restricted to the Critical Location, the Foreign Location, and the Developer site.

A.7 Detailed Evaluation Description

320 The Evaluator SHALL present an evaluation schedule that identifies the total amount of planned effort required to perform the work for each work item.

321 The Evaluator SHALL demonstrate to the Certification Body that the plan is achievable with the allocated resources. For example, concurrently assigning the same evaluators to two or more different work items may indicate a risk to completing the evaluation work as planned.

322 The Evaluator SHALL present details regarding the Evaluator's approach to independent testing, as well as the Evaluator's approach to vulnerability analysis (assuming this is part of the evaluation). The level of detail expected shall be sufficient to provide the Certifier with confidence that the Evaluator has performed enough preliminary investigation to determine the scope and magnitude of the independent testing and vulnerability analysis.

323 The Evaluator SHALL demonstrate to the Certification Body that the Evaluator recognises and has considered the increasing evaluation work complexity as the EAL increases. This applies to all evaluation work including work units that are consistent across all EAL levels.

Appendix B Test Planning Meeting

B.1 Overview

324 The Lead Certifier and/or the Evaluator may propose a voluntary test planning meeting. The meeting should take place at least five working days before the test monitoring and the penetration testing for the assurance classes tests (ATE) and vulnerability analysis (AVA).

325 The purpose is to focus on planning more than monitoring and to give the Evaluator enough time to adjust the testing in accordance to the outcome of the meeting. The goal of the meeting is that the Evaluator presents and justifies the test plan in order to reduce the risk that further tests need to be carried out due to shortcomings in the planning stage.

B.2 Input

326 A preliminary test plan should be passed as input no later than five working days prior to the meeting, which includes answers to who, where, what products and which variants that are planned to be tested, what functionality and how these are planned to be tested. If any relevant functionality is excluded from testing it should also be described and justified. A draft mapping between tests and Security Functional Requirements (SFR) should be included to show the structure that is to be used in the final mapping.

327 The Evaluator´s strategy for the planning of tests:

- Evaluator´s planned choice of repeating Developer tests- coverage
- Evaluator´s planned choice of independent testing - justification
- Evaluator´s planned choice of penetration tests - justification
- if there in rare cases are tests the Evaluator chose not to perform - motivation
- Evaluator´s test methodology- justification that the proposed tests are appropriate for the intended functionality

B.3 Output

328 The output of the test planning meeting's is preparatory work for the review for the ATE and AVA reports. No final review is made at the test planning meeting and the Lead Certifier assesses on a case by case basis if the test monitoring is to be done too. The preliminary test plan should demonstrate that the Evaluators intentions are reasonable, but full compliance with CC and CEM will be verified by reviewing the assurance class tests (ATE) and vulnerability (AVA) reports. During a test planning meeting the Certifier will not make any final reviews concerning the adequacy of the tests. The final assessment is made in connection with ATE-and AVA-reports.

Appendix C Single Evaluation Report

C.1 Overview

329 The Evaluator documents the interim verdicts and justifications in accordance with the CEM in a single evaluation report. A single evaluation report covers a subset of all assurance packages for the evaluation. For larger assurance classes, each assurance family can be covered in a separate single evaluation report.

C.1.1 Protection Profile Evaluation

330 For protection profile evaluations the single evaluation report is used without a final evaluation report and therefore the single evaluation report must provide information necessary to produce the certification report.

C.2 Structure and Information Content

331 The following requirements apply to a single evaluation report in general. At a minimum, the cover page SHOULD contain the following information.

- Document name
- Version number
- File name
- Product name
- Sponsor name
- ITSEF name
- Certification Body name
- Certification ID
- Lead Evaluator name
- Appropriate protective markings

332 At a minimum, the headers or footers of all pages following the cover page SHOULD identify the following.

- Certification ID
- Appropriate protective markings
- Page number

333 The single evaluation report SHOULD be structured by the following section headings.

1. Evaluation Basis and Documents
2. Objectives and Dependencies
3. Evaluation Evidence and Work Units
4. Evaluation Result
5. References
6. Abbreviations and Glossary

334 The content requirements SHOULD be met in the sections included in the single evaluation report. The single evaluation report MAY include additional sections, structured as appropriate, complying with the single evaluation report purpose.

335 The information content requirements follow.

C.2.1 Evaluation Basis and Documents

336 The evaluation basis SHALL identify the following.

- CC version
- Evaluation methodology
- Security target (ST)

337 The evaluation basis SHALL also identify the following.

- Relevant Scheme documents
- Interpretations considered for this single evaluation report
- Sponsor and/or Developer documents provided for the evaluation aspects addressed in this single evaluation report
- All applicable supporting documents with relevant versions indicated

C.2.2 Objectives and Dependencies

338 The objectives for this assurance class or assurance family SHOULD be identified and described, including the following.

- EAL
- Dependencies taken into account during the evaluation

C.2.3 Evaluation Evidence and Work Units

339 This section SHOULD identify the following.

- Evaluator action elements
- Content and presentation of evaluation evidence elements
- Applicable work units

340 When several Evaluators have been working on the report and the result will be used for collecting merits for Qualified Evaluator status this section SHOULD clearly identify which work units or parts of work units each involved Evaluator conducted.

C.2.4 Evaluation Result

341 The evaluation result section is the major part of the single evaluation report. This section SHALL contain, preferably presented in a table, the interim verdicts for:

- the assurance class,
- the assurance components,
- the evaluator action elements, and
- the work units.

342 For each work unit, the evaluation result section SHALL provide the following:

- Unique identification of the work unit
- Identification of the evaluation input and a brief description of the information provided by the Sponsor and/or Developer relevant to this work unit
- Necessary argumentation and a conclusion, based on the evaluation evidence and the evaluation work performed, why the requirements of the work unit are fulfilled (or why not). The description has to be detailed enough to make the conclusion obvious for the reader, in order to ensure general repeatability and reproducibility,
- Evaluator's interim verdict for this work unit

343 The single evaluation report SHOULD also identify the following:

- Consideration of vulnerabilities, in which the Evaluator describes all potential vulnerabilities found during the evaluation covered by the single evaluation report
- Impact on other documents identified during this evaluation

C.2.5 References

344 The list of references SHALL contain a complete listing of all documents used during the evaluation and referred to in the single evaluation report.

345 The Evaluation reports SHALL contain information about any technical experts, other experts or Evaluator assistants who have contributed to the evaluation and it SHOULD be clarified in the report which parts they have contributed with.

346 Documents should be referenced using the following format:
Title (incl. product name & version if applicable), Document version x.x, Issuing organisation, Date, Document id (optional).

Example:
EP-002 *Evaluation and Certification*, document version 20.0, CSEC, 2013-09-30, FMV ID 13FMV7990-2:1.

C.2.6 Abbreviations and Glossary

347 This section SHOULD expand on acronyms or abbreviations and define any specialised terms used in the single evaluation report that are not considered common knowledge. The acronyms and abbreviations list and glossary may be a part of the single evaluation report or may be maintained as a separate document referenced by the single evaluation report.

Appendix D Final Evaluation Report

D.1 Overview

348 The final evaluation report covers all evaluation activities in all single evaluation reports. The objective of the final evaluation report is to provide the overall verdict with justification, and to provide information necessary to produce the certification report.

349 The Evaluation section in the final evaluation report contains detailed information about the evaluation. The Results of the Evaluation section contains references to the single evaluation reports. A brief summary of the evaluation results is given in the Executive Summary.

350 With the exception of the detailed evaluation information mentioned above, the final evaluation report should not contain information not suited to be copied into the certification report.

D.2 Structure and Information Content

351 The following requirements apply to the final evaluation report in general. At a minimum, the cover page SHOULD contain the following information.

- Document title
- Version number
- File name
- Product name
- Sponsor name
- ITSEF name
- Certification Body name
- Certification ID
- Lead Evaluator name
- Appropriate protective markings

352 At a minimum, the headers or footers of all pages following the cover page SHOULD identify the following.

- Certification ID
- Appropriate protective markings
- Page number

353 The final evaluation report SHOULD be structured by the following section headings.

1 Introduction
  1.1 Executive Summary
  1.2 Identification of the target of evaluation
  1.3 Security Target
2 Architectural Description of the target of evaluation
3 Evaluation
4 Results of the Evaluation
5 Evaluator Comments, Observations and Recommendations
6 References
7 Glossary
A Annexes

354 The content requirements SHOULD be met in the sections included in the final evaluation report. The final evaluation report MAY include additional sections, structured as appropriate, providing they comply with the final evaluation report purpose.

355 In the case of a protection profile evaluation, the same structure SHOULD be used; however, non-relevant sections SHOULD be marked “Not applicable” or be omitted.

356 The final evaluation report content requirements are described in the following sections.

D.2.1 Executive Summary

357 The executive summary SHOULD be a brief summary of the entire report. The information contained within this section SHOULD provide the audience with a clear and concise overview of the target of evaluation and of the evaluation results. This section SHOULD include all key evaluation findings.

358 The reader of this section SHOULD gain a basic understanding of the evaluated product's functionality, as well as the results of the evaluation.

359 The executive summary SHOULD contain, but is not limited to, the following items.

- Name of the evaluated target of evaluation
- Target of evaluation version identifier
- An enumeration of the components of the target of evaluation that are part of the evaluation
- The name of the Scheme: "Swedish Common Criteria Evaluation and Certification Scheme"
- Developer name
- Sponsor name
- ITSEF name
- Completion date of the evaluation
- Brief description of the report results

360 The executive summary SHOULD also contain a summary of the following.

- Evaluation assurance package
- Conformance claims to protection profiles
- Security functionality
- Threats and organisational security policies addressed by the evaluated target of evaluation
- Special or unusual configuration requirements
- Special or unusual assumptions about the operating environment

D.2.2 Identification of the Target of Evaluation

361 The evaluated target of evaluation SHALL be clearly identified. The version number of all separate software modules in the target of evaluation, applicable software patches, hardware, and peripheral devices SHOULD be identified. All documentation, included when the target of evaluation is delivered to a customer, SHOULD also be uniquely identified.

362 All labelling and descriptive information necessary to completely identify the target of evaluation SHALL be given here. Complete identification of the target of evaluation will ensure that a whole and accurate representation of the target of evaluation can be recreated for use or for future evaluation efforts.

D.2.3 Security Target

363 The security target, possibly a sanitised version, SHALL be referenced in this section.

D.2.4 Architectural Information

364 This section SHOULD provide a functional decomposition of the target of evaluation in terms of its major hardware and software structures. Significant data flows between these structures SHOULD also be identified and described as necessary to understand how the data is used in the context of the security policy.

365 If the evaluation assurance requirements include any assurance components from the assurance class development, target of evaluation design (ADV_TDS) family, then the target of evaluation architectural description SHOULD be based on the Evaluator's understanding of the high-level design; but this section SHOULD contain neither a complete reproduction of, nor simply a reference to, the high-level design.

366 If a high-level design is not available because no ADV_TDS component is included in the evaluation assurance package, then the architectural description SHOULD be based on the Evaluator's understanding of other evaluation evidence available to the Evaluator, particularly the functional specification.

D.2.5 Evaluation

367 This section SHOULD define the evaluation in terms of evaluation methods, techniques, tools and standards used. In particular, it SHOULD be made clear which version of the evaluation criteria and evaluation methodology has been used, as well as which interpretations have been taken into account. Also, devices used to perform the tests SHOULD be mentioned.

368 If any constraints apply to the evaluation, such as special circumstances or assumptions made during the evaluation that have an impact on the evaluation results, it SHOULD be reported here. Other relevant information, related to legal aspects, confidentiality requirements MAY also be presented in this section.

369 The final evaluation report SHALL identify all locations where evaluation activities have been performed. (See EP-191 *Cross Frontier Evaluation*.)

D.2.6 Results of the Evaluation

370 This section SHALL provide the overall verdict for the evaluation as defined in Common Criteria Part 1 *Introduction and general model,* section 7, General Model, based on the Evaluator's interim verdict for each Evaluator action element, each assurance component, and each assurance class.

371 Also, in this section, a reference to each single evaluation report SHOULD be given, where detailed descriptions of the evaluation may be found.

D.2.7 Evaluator Comments, Observations, and Recommendations

372 Additional information of possible interest to potential users acquired by the Evaluator during the course of the evaluation SHOULD be documented in this section.

373 This section may include information on shortcomings of the target of evaluation that did not have an impact on the evaluation results, or information helpful in using the product more securely.

374 This section SHOULD include a complete list of all observation reports submitted during the evaluation and their status.

D.2.8 References

375 This section SHALL list all referenced documentation used as source material in the compilation of the report. This information SHOULD include, but not be limited to the following.

- Applicable versions of the Common Criteria (CC Part 1-5 refers to the Common Criteria standard documentation) and Common Methodology for Information Technology Security Evaluation (CEM)
- Applicable Certification Body documentation
- Technical reference documentation
- A complete listing of evaluation evidence used in the evaluation
- A complete list of any technical experts, other experts or Evaluator assistants who have contributed to the evaluation

376 Documents should be referenced using the following format:
Title (incl. product name & version if applicable), Document version x.x, Issuing organisation, Date, Document id (optional).

Example:
EP-002 *Evaluation and Certification*, document version 20.0, CSEC, 2013-09-30, FMV ID 13FMV7990-2:1.

D.2.9 Glossary

377 The glossary SHOULD be used to increase the readability of the report by providing definitions of acronyms or terms of which the meanings may not be readily apparent.

D.2.10 Annexes

378 The annexes MAY be used to outline any additional information that may be useful to the reader but does not logically fit within the prescribed headings of the report.

Appendix E Impact Analysis Report

379 This section describes the minimum content of the impact analysis report (IAR). The contents are portrayed in Figure 2; this figure may be used as a guide when constructing the structural outline of the document. The Impact Analysis Report is a required input for the assurance continuity process.

380 Throughout the following description, for "the Developer" read "the Developer or the ITSEF on behalf of the Developer".

Figure 3. Impact analysis report information content

E.1 Introduction

381 The Developer SHALL report the impact analysis report configuration control identifiers.

- *The impact analysis report configuration control identifiers contain information that identifies the impact analysis report (e.g. name, date and version number).*

382 The Developer SHALL report the current target of evaluation configuration control identifiers.

- *The target of evaluation configuration control identifiers identify the current version of the target of evaluation that reflects changes to the certified target of evaluation.*

383 The Developer SHALL report the configuration control identifiers for the final evaluation report, certification report, and the certified target of evaluation.

- *These configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.*

384 The Developer SHALL report the configuration control identifiers for the version of the security target related to the certified target of evaluation.

385 The Developer SHALL report the identity of the Developer.

- *The identity of the target of evaluation Developer is required to identify the party responsible for producing the target of evaluation, performing the impact analysis and updating the evidence.*

386 The Developer MAY include information in relation to legal or statutory aspects, for example related to the confidentiality of the document.

E.2 Description of the Change(s)

387 The Developer SHALL report the changes to the product.

- *The identified changes are with regard to the product associated with the certified target of evaluation.*

388 The Developer SHALL report the changes to the development environment.

- *The identified changes are with regard to the development environment of the certified target of evaluation.*

E.3 Affected Developer Evidence

389 For each change, the Developer SHALL report the list of affected items of the developer evidence.

- For each change to the product associated with the certified target of evaluation or to the development environment of the certified target of evaluation, any item of the developer evidence that need to be modified in order to address the Developer action elements SHALL be identified.

E.4 Description of the Developer Evidence Modifications

390 The Developer SHALL describe briefly the required modifications to the affected items of the developer evidence.

- For each affected item of the developer evidence, the modifications required to address the corresponding content and presentation of evidence elements SHALL be briefly described.

E.5 Conclusions

391 For each change the Evaluator SHALL report if the impact on assurance is considered minor or major.

- For each change the Evaluator SHOULD provide a supporting rationale for the reported impact. In the event that the change is to the development environment, the rationale SHOULD show that there is no follow-on impact on other assurance measures.

392 The Evaluator SHALL report if the overall impact is considered minor or major.

- The Evaluator SHOULD include a supporting rationale, taking the accumulation of changes into consideration.

E.6 Annex: Updated Developer Evidence

393 The Developer SHALL report for each updated item of developer evidence the following information:

- the title;
- the unique reference (e.g. issue date and version number).

- *Only those items of evidence that are notably changed need to be listed; if the only update to an item of evidence is to reflect the new identification of the target of evaluation, then it does not need to be included.*